(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 July 2005 (07.07.2005)

PCT

(10) International Publication Number
WO 2005/062523 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/KR2004/001911

(22) International Filing Date: 29 July 2004 (29.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2003-0095373
23 December 2003 (23.12.2003) KR

(71) Applicant *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161, Gajeong-dong, Yusong-gu, Daejeon-city 305-350 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JEON, Yong-Sung** [KR/KR]; 112-1005 Hwangsiltown Apt., 302, Wolpyung-dong, Seo-gu, Daejeon-city 302-280 (KR). **PARK, Ji-Man** [KR/KR]; 310-1208 Cheongsol Apt., Songgang-dong, Yusong-gu, Daejeon-city 305-752 (KR). **PARK, Young-Soo** [KR/KR]; 101-907 Sanho Apt., Tanbang-dong, Seo-gu, Daejeon-city 302-766 (KR). **JUN, Sung-Ik** [KR/KR]; 107-704 Hanbit Apt., Eoeun-dong, Yusong-gu, Daejeon-city 305-755 (KR). **CHUNG, Kyo-Il** [KR/KR]; 107-1102 Hanwool Apt., Shinsung-dong, Yusong-gu, Daejeon-city 305-707 (KR).

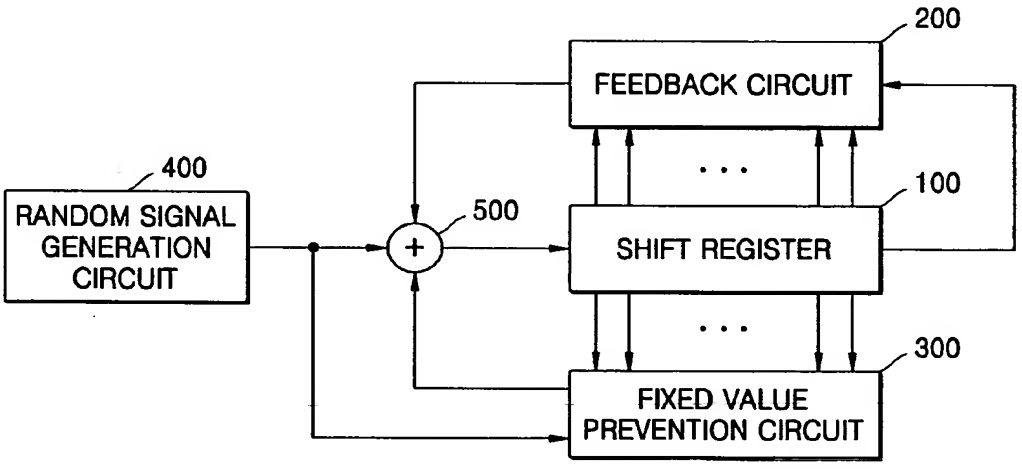
(74) Agent: **LEE, Young-Pil**; The Cheonghwa Building, 1571-18 Seocho-dong, Seocho-gu, Seoul 137-874 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR GENERATING RANDOM NUMBER USING DIGITAL LOGIC



(57) Abstract: An apparatus and method for generating random numbers using digital logic are provided. The apparatus includes a shift register which sequentially moves bit values stored therein, a feedback circuit which performs a predetermined logic operation on the bit values stored in the shift register to generate a feedback signal, an external signal generation circuit which generates an external signal input to the shift register, and an input logic circuit which performs a predetermined logic operation on the feedback signal and the external signal and inputs a result of operation to the shift register. The method includes sequentially moving bit values stored in a shift register, (b) performing a predetermined logic operation on the bit values stored in the shift register to generate a feedback signal, (c) generating an external signal input to the shift register, and (d) performing a predetermined operation on the feedback signal and the external signal and inputting a result of the operation to the shift register.

WO 2005/062523 A1

FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *with amended claims and statement*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.